Abstract

The present invention discloses a construction for key management module functionality which provides for secure encoding and decoding of messages which are up to two blocks long. A method for generating an encoded value having a first encoded value part and a second encoded value part from an unencoded value having a first unencoded value part and a second unencoded value part, comprising the steps of: obtaining an initialization vector; and generating the first and second encoded value parts. The first encoded value part is generated by: generating a first result by encrypting the first unencoded value part; generating a second result by performing an exclusive or operation on the first result and the second unencoded value part; generating a third result by performing an exclusive or operation on the second result and the initialization vector; generating a fourth result by encrypting the third result; generating a fifth result by performing an exclusive or operation on the fourth result and the first unencoded value part; and encrypting the fifth result. The second encoded value part is generated by encrypting the second result.